FORT HOOD COMPUTER USER AGREEMENT

As a user of an automated information system at Fort Hood, I will adhere to the following:

1. I will use Government information systems (computers, systems and networks) only for authorized purposes. I understand that access to Army resources is a revocable privilege and is subject to content monitoring and security testing.
2. I will not install any unlicensed, unaccredited or unapproved software on any Government system (computer, system or network). If such is required, I will contact my IASO or SA.
3. I will not install/connect any hardware on any Government system (computer, system or network). If such is required, I will contact my IASO or SA.
4. I will not try to access data or use operating systems or programs, except as specifically authorized.
5. I will be issued a user identifier (user ID) and a password to authenticate my computer account. After receiving them:
    a. I understand that I am the only authorized user of this account. I will not allow anyone else to have or use my password. If I know my password has been compromised, I will report this to the IASO.
    b. I am responsible for all activities that occur on my individual account once my password has been issued to me.
    c. I will ensure that my password is changed every 150 days (if unclassified), or every 90 days (if classified) or if compromised, whichever is sooner.
    d. I understand that I will generate, store, and protect passwords. Passwords will consist of at least 10 characters with 2 each of uppercase, and lowercase letters, numbers, and special characters. I will not use my user ID, common names, birthdays, phone numbers, military acronyms, call signs or dictionary words as passwords.
    e. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.
    f. I will not store my password on any processor, computer, personal digital assistant (PDA), personal electronic device (PED) or any magnetic or electronic media.
    g. I will not tamper with my computer to avoid adhering to the Fort Hood security policies.
6. I know that it is a violation of policy for any computer to try to mask his/her identity, or to try to assume the identity of someone else.
7. I will scan all magnetic media (disks, CDs etc.) for malicious software (i.e. viruses, worms) before using it on an IS connected or disconnected from an Army and/or Fort Hood network.
8. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO and delete the message.
9. I will not run "sniffer" or any hacker-related software on any Government system (computer, system or network).
10. I will not download file-sharing software (including MP3 music and video files) or games onto any Government system (computer, system or network).
11. I will not connect any personal IT equipment (PDAs, PEDs) to my computer, or a personal computer to the Fort Hood network, without written approval by the Ft. Hood IAM and DAA.
12. I will ensure that my anti-virus software on my computer is updated at least weekly.
13. I will not use Internet Chat or instant messenger services (i.e. AOL, MSN, Yahoo) from my IS. If chat service is required, I will use the chat service established with my AKO account.
14. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify my IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.
15. I will use a password-protected screensaver and log off the workstation when departing the area.
16. I will comply with the security guidance issued by the Fort Hood IAM, and my IASO and SA.
17. If I have a public key infrastructure (PKI) certificate installed on my computer (i.e. software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.

18. I understand that each IS is the property of the US Government and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

19. I know that if connected to the Secret Internet Protocol Router Network (SIPRNET), my system operates at least in the U.S. Secret, "system-high" mode.

a. Any magnetic media used on the system must be immediately classified and protected at the system-high level, regardless of the implied classification of the data (until declassified or downgraded by an approved process).

b. I must properly protect all material printed out from the SIPRNET.

c. I will not enter information into a system if the information has a higher classification than that for which the system is rated. I will not enter information that is proprietary, contractor-excluded, or otherwise needs special protection or handling, unless approved in writing by the IASO.

d. I will have the appropriate clearance necessary to access the system.

e. Magnetic and compact disks will not be removed form the computer area without the approval of the local commander or director.

20. My local IASO has informed me of the TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections.

21. I understand this agreement and will keep the computer secure. If I am the site supervisor, group chief, IASO, or SA, I will ensure that all users in my area of responsibility sign this agreement.

22. I know I am subject to disciplinary action if I violate the Fort Hood computer security policy. If I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.

This agreement must be signed by both parties prior to issuance of a network account and password. The IASO will retain a copy of each user's agreement until the individual no longer requires network access.

User Name: _____

User Signature: _____

Date: _____

IASO Name: _____

IASO Signature: _____

Date: _____